

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号
特開2000-98885
(P2000-98885A)

(43) 公開日 平成12年4月7日(2000.4.7)

(51) Int.Cl. ⁷	識別記号	F I	テーマコード [*] (参考)
G 0 9 C 1/00	6 2 0	G 0 9 C 1/00	6 2 0 A 5 B 0 1 7
G 0 6 F 12/14	3 2 0	G 0 6 F 12/14	3 2 0 B 5 J 1 0 4
H 0 4 L 9/00		H 0 4 L 9/00	6 0 1 D

審査請求 未請求 請求項の数41 O L (全 16 頁)

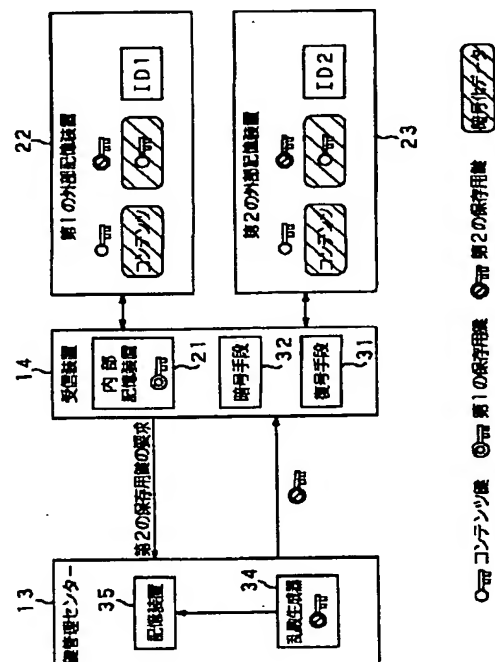
(21) 出願番号	特願平10-263694	(71) 出願人	000002185 ソニー株式会社 東京都品川区北品川6丁目7番35号
(22) 出願日	平成10年9月17日(1998.9.17)	(72) 発明者	石橋 義人 東京都品川区北品川6丁目7番35号 ソニー株式会社内
		(74) 代理人	100067736 弁理士 小池 晃 (外2名) Fターム(参考) 5B017 AA06 AA07 BA05 BA07 BB10 CA16 5J104 AA12 AA16 EA02 EA17 MA05 NA02 NA27 NA37 PA14

(54) 【発明の名称】 コンテンツ管理方法及びコンテンツ記憶システム

(57) 【要約】

【課題】 本発明は、コンテンツの不正コピーを防止しながらそのバックアップを生成することを可能にするコンテンツ管理方法の提供を目的としている。

【解決手段】 受信装置14は、第1の保存用鍵により暗号化されているコンテンツ鍵と、コンテンツ鍵により暗号化されているコンテンツとを記憶する第1の外部記憶装置22と、復号手段31において第1の保存用鍵により復号して得たコンテンツ鍵を、乱数生成器34により生成した第2の保存用鍵により暗号手段32において暗号化して得た暗号化されたコンテンツ鍵と、暗号化されているコンテンツとを記憶する第2の外部記憶装置23とを備えている。



1

【特許請求の範囲】

【請求項1】 コンテンツを記憶するための複数のコンテンツ記憶手段を備えるデータ記憶装置におけるコンテンツ管理方法であって、

第1の保存用鍵により暗号化されたコンテンツ鍵と、コンテンツ鍵により暗号化されているコンテンツとを記憶している第1のコンテンツ記憶手段の当該暗号化されているコンテンツ鍵を第1の保存用鍵により復号し、復号して得たコンテンツ鍵を、新たに生成した第2の保存用鍵により暗号化し、

上記第2の保存用鍵により暗号化されたコンテンツ鍵と上記暗号化されているコンテンツとを上記第2のコンテンツ記憶手段に記憶することを特徴とするコンテンツ管理方法。

【請求項2】 乱数に基づいて上記第2の保存用鍵を生成することを特徴とする請求項1記載のコンテンツ管理方法。

【請求項3】 上記復号して得たコンテンツ鍵を、上記第2の保存用鍵及び上記第2のコンテンツ記憶手段の識別情報により暗号化して上記第2のコンテンツ記憶手段に記憶することを特徴とする請求項1記載のコンテンツ管理方法。

【請求項4】 上記コンテンツ鍵は、上記第1のコンテンツ記憶手段において、上記第1の保存用鍵及び上記第1のコンテンツ記憶手段の識別情報により暗号化されており、

上記第1のコンテンツ記憶手段に記憶されているコンテンツ鍵は、上記第1の保存用鍵及び上記第1のコンテンツ記憶手段の識別情報により復号されることを特徴とする請求項1記載のコンテンツ管理方法。

【請求項5】 上記第2の保存用鍵は、上記データ記憶装置の備える復号鍵生成手段により生成されることを特徴とする請求項1記載のコンテンツ管理方法。

【請求項6】 保存用鍵を管理する鍵管理装置用の公開鍵により第2の保存用鍵を暗号化して第3の保存用鍵を生成し、

上記第3の保存用鍵を上記第2のコンテンツ記憶手段に記憶することを特徴とする請求項5記載のコンテンツ管理方法。

【請求項7】 上記データ記憶装置は、上記第2のコンテンツ記憶手段への上記第3の保存用鍵の記憶に応じて上記第2の保存用鍵を削除することを特徴とする請求項6記載のコンテンツ管理方法。

【請求項8】 上記データ記憶装置は、上記第2のコンテンツ記憶手段に記録されているコンテンツ鍵を復号する際に、上記鍵管理装置に上記第3の保存用鍵を送信し、

上記鍵管理装置は、上記第3の保存用鍵に基づいて第2の保存用鍵を生成するとともに、所定の課金手順に従って課金処理することを特徴とする請求項7記載のコンテンツ

2

管理方法。

【請求項9】 上記第2の保存用鍵は、保存用鍵を管理する鍵管理装置が備える保存用鍵生成手段により生成され、

上記鍵管理装置には、上記第2の保存用鍵と、この生成された第2の保存用鍵により暗号化されるコンテンツ鍵が記憶される第2のコンテンツ記憶手段の識別情報とが保存されることを特徴とする請求項1記載のコンテンツ管理方法。

10 【請求項10】 上記鍵管理装置は、第2の保存用鍵の生成に応じて所定の課金手順に従って課金処理すること

を特徴とする請求項9記載のコンテンツ管理方法。

【請求項11】 上記鍵管理装置は、管理用鍵により上記第2の保存用鍵を暗号化して第3の保存用鍵を生成して、この第3の保存用鍵を上記データ記憶装置に送信し、

上記データ記憶装置は、上記第2のコンテンツ記憶手段に上記第3の保存用鍵を記憶することを特徴とする請求項9記載のコンテンツ管理方法。

20 【請求項12】 上記データ記憶装置は、上記第2のコンテンツ記憶手段へ上記第3の保存用鍵の記憶に応じて上記第2の保存用鍵を削除することを特徴とする請求項11記載のコンテンツ管理方法。

【請求項13】 上記鍵管理装置は、上記第2の保存用鍵により暗号化されたコンテンツ鍵が記憶されている第2のコンテンツ記憶手段の識別情報を保存しており、上記データ記憶装置は、第2のコンテンツ記憶手段に記憶されているコンテンツ鍵を復号する際に、上記鍵管理装置に上記第2のコンテンツ記憶手段の識別情報を送信し、

30 上記鍵管理装置は、上記データ記憶装置から送られてきた上記第2のコンテンツ記憶手段の識別情報と自己が保持している上記第2のコンテンツ記憶手段の識別情報との比較結果に基づいて第2の保存用鍵を生成するとともに、所定の課金手順に従って課金処理することを特徴とする請求項12記載のコンテンツ管理方法。

【請求項14】 上記第2のコンテンツ記憶手段には、上記データ記憶装置の識別情報が記憶されていることを特徴とする請求項1記載のコンテンツ管理方法。

40 【請求項15】 上記データ記憶装置は、上記第2のコンテンツ記憶手段に記憶されているデータ記憶装置の識別情報の検査結果に応じて、当該第2のコンテンツ記憶手段に記憶されているコンテンツ鍵の復号を開始することを特徴とする請求項14記載のコンテンツ管理方法。

【請求項16】 上記第2のコンテンツ記憶手段から復号して得た上記コンテンツ鍵にはこのコンテンツ鍵が復旧により得ている旨の情報を付加することを特徴とする請求項1記載のコンテンツ管理方法。

50 【請求項17】 上記データ記憶装置は、復旧により得ている旨が付加されているコンテンツ鍵を移動する際

3

に、このコンテンツ鍵と移動先に保存されているコンテンツ鍵との比較した比較結果に基づいてエラー処理することを特徴とする請求項 16 記載のコンテンツ管理方法。

【請求項 18】 コンテンツ鍵の使用可能回数を制限する使用回数情報が上記コンテンツ鍵に付加されていることを特徴とする請求項 1 記載のコンテンツ管理方法。

【請求項 19】 上記第 2 のコンテンツ記憶手段に上記第 1 のコンテンツ記憶手段のコンテンツ鍵と共に当該第 1 のコンテンツ記憶手段の識別情報を記憶し、上記第 2 のコンテンツ記憶手段に記憶されているコンテンツ鍵を復号した際には、この第 2 のコンテンツ記憶手段に記憶されている上記識別情報をデータ記憶装置において保存し、

データ記憶装置は、上記第 1 のコンテンツ記憶手段のコンテンツ鍵の復号の要求があった際には、この要求があった当該第 1 のコンテンツ記憶手段の識別情報と上記第 2 のコンテンツ記憶手段からの上記識別信号とを比較した比較結果に基づいてエラー処理することを特徴とする請求項 1 記載のコンテンツ管理方法。

【請求項 20】 第 1 の保存用鍵により暗号化されているコンテンツ鍵と、コンテンツ鍵により暗号化されているコンテンツとを記憶している第 1 のコンテンツ記憶手段と、

データ及び鍵データを復号する復号手段と、
データ及び鍵データを暗号化する暗号手段と、
保存用鍵を生成する保存用鍵生成手段と、
上記復号手段において上記第 1 の保存用鍵により復号して得たコンテンツ鍵を、上記保存用鍵生成手段により生成した第 2 の保存用鍵により上記暗号手段において暗号化して得た暗号化されたコンテンツ鍵と、上記暗号化されているコンテンツとを記憶する第 2 のコンテンツ記憶手段と、
保存用鍵が記憶されている保存鍵記憶手段とを備えることを特徴とするコンテンツ記憶システム。

【請求項 21】 上記保存用鍵生成手段は、乱数発生器により上記第 2 の保存用鍵を生成することを特徴とする請求項 20 記載のコンテンツ記憶システム。

【請求項 22】 上記第 2 のコンテンツ記憶手段には、上記復号手段において復号して得たコンテンツ鍵を、上記第 2 の保存用鍵及び上記第 2 のコンテンツ記憶手段の識別情報により上記暗号手段において暗号化して得たコンテンツ鍵が記憶されることを特徴とする請求項 20 記載のコンテンツ記憶システム。

【請求項 23】 上記コンテンツ鍵は、上記第 1 のコンテンツ記憶手段において、上記第 1 の保存用鍵及び上記第 1 のコンテンツ記憶手段の識別情報により暗号化されており、
上記第 1 のコンテンツ記憶手段に記憶されているコンテンツ鍵は、上記第 1 の保存用鍵及び上記第 1 のコンテン

4

ツ記憶手段の識別情報により復号されることを特徴とする請求項 20 記載のコンテンツ記憶システム。

【請求項 24】 上記第 1 のコンテンツ記憶手段、上記復号手段、上記暗号手段、上記第 2 のコンテンツ記憶手段、上記保存用鍵記憶手段及び上記保存用鍵生成手段はデータ記憶装置を構成しており、
上記データ記憶装置の保存用鍵を管理する鍵管理装置をさらに備えていることを特徴とする請求項 20 記載のコンテンツ記憶システム。

10 【請求項 25】 上記データ記憶装置は、データ送信装置から暗号化されて送信されてくるコンテンツを受信するデータ受信装置であることを特徴とする請求項 24 記載のコンテンツ記憶システム。

【請求項 26】 上記鍵管理装置用の公開鍵を記憶する公開鍵記憶手段を備えており、
上記第 2 のコンテンツ記憶手段には、上記第 2 の保存用鍵と共に上記公開鍵によりこの第 2 の保存用鍵を暗号化して得た第 3 の保存用鍵が記憶されていることを特徴とする請求項 24 記載のコンテンツ記憶システム。

20 【請求項 27】 上記データ記憶装置は、上記第 2 のコンテンツ記憶手段に上記第 3 の保存用鍵が記憶されたことに応じて上記第 2 の保存用鍵を削除することを特徴とする請求項 26 記載のコンテンツ記憶システム。

【請求項 28】 上記データ記憶装置は、上記第 2 のコンテンツ記憶手段に記憶されているコンテンツ鍵を復号する際には、上記鍵管理装置に対して上記第 3 の保存用鍵を送信し、

上記鍵管理装置は、上記第 3 の保存用鍵に基づいて生成した第 2 の保存用鍵をデータ送信装置に送信するとともに、
30 所定の課金手順に従って課金処理することを特徴とする請求項 27 記載のコンテンツ記憶システム。

【請求項 29】 上記第 2 のコンテンツ記憶手段には、上記データ記憶装置の識別情報が記憶されていることを特徴とする請求項 24 記載のコンテンツ記憶システム。

40 【請求項 30】 上記データ記憶装置は、上記第 2 のコンテンツ記憶手段に記憶されているデータ記憶装置の識別情報の検査結果に応じて、当該第 2 のコンテンツ記憶手段に記憶されているコンテンツ鍵の復号処理を開始することを特徴とする請求項 29 記載のコンテンツ記憶システム。

【請求項 31】 上記第 1 のコンテンツ記憶手段、上記復号手段、上記暗号手段、上記第 2 のコンテンツ記憶手段及び上記保存用鍵記憶手段はデータ記憶装置を構成しており、

上記保存用鍵生成手段を有して、上記データ記憶装置の保存用鍵を管理する鍵管理装置をさらに備えていることを特徴とする請求項 20 記載のコンテンツ記憶システム。

50 【請求項 32】 上記データ記憶装置は、データ送信装置から暗号化されて送信されてくるコンテンツを受信す

5

るデータ受信装置であることを特徴とする請求項31記載のコンテンツ記憶システム。

【請求項33】 上記鍵管理装置は、鍵管理装置が生成した保存用鍵と、この生成された保存用鍵により暗号化されるコンテンツ鍵が記憶されるコンテンツ記憶手段の識別情報とが保存される識別情報記憶手段を備えていることを特徴とする請求項31記載のコンテンツ記憶システム。

【請求項34】 上記鍵管理装置は、保存用鍵の生成に応じて所定の課金手順に従って課金処理を行うことを特徴とする請求項31記載のコンテンツ記憶システム。

【請求項35】 上記鍵管理装置は、管理用鍵を記憶する管理用鍵記憶手段を備え、
上記鍵管理装置は、上記管理用鍵により上記第2の保存用鍵を暗号化して第3の保存用鍵を生成し、当該第3の保存用鍵を上記データ記憶装置へ送信し、
上記データ記憶装置は、上記第2のコンテンツ記憶手段に上記第3の保存用鍵を記憶することを特徴とする請求項31記載のコンテンツ記憶システム。

【請求項36】 上記データ記憶装置は、上記第2のコンテンツ記憶手段に上記第3の保存用鍵が記憶されたことに応じて上記第2の保存用鍵を削除することを特徴とする請求項35記載のコンテンツ記憶システム。

【請求項37】 上記鍵管理装置は、上記第2の保存用鍵と、この第2の保存用鍵により暗号化されるコンテンツ鍵が記憶される第2のコンテンツ記憶手段の識別情報とを保存する識別情報記憶手段を備え、
上記鍵管理装置は、上記データ記憶装置がコンテンツ鍵を復号する際に、このデータ記憶装置から送られてきた上記第2のコンテンツ記憶手段の識別情報と上記識別情報記憶手段に記憶されている上記識別情報との比較結果に基づいて所定の課金手順に従って課金処理することを特徴とする請求項36記載のコンテンツ記憶システム。

【請求項38】 上記第2のコンテンツ記憶手段には、上記データ記憶装置の識別情報が記憶されていることを特徴とする請求項31記載のコンテンツ記憶システム。

【請求項39】 上記データ記憶装置は、上記第2のコンテンツ記憶手段に記憶されているコンテンツ鍵の復号を開始することを特徴とする請求項38記載のコンテンツ記憶システム。

【請求項40】 上記第2のコンテンツ記憶手段から復号して得たコンテンツ鍵にはこのコンテンツ鍵が復旧により得ている旨の情報が使用条件情報として付加されていることを特徴とする請求項20記載のコンテンツ記憶システム。

【請求項41】 コンテンツ鍵の使用可能回数を制限する使用回数情報がコンテンツ鍵に付加されていることを特徴とする請求項20記載のコンテンツ記憶システム。

【発明の詳細な説明】

【0001】

6

【発明の属する技術分野】本発明は、コンテンツを記憶手段に記憶して管理するコンテンツ管理方法及びコンテンツ記憶システムに関して、詳しくは、複数の記憶手段に対してコンテンツを記憶するデータ記憶装置に好適なコンテンツ管理方法及びコンテンツ記憶システムに関する。

【0002】

【従来の技術】近年、衛星放送やインターネット等を用いた電子配信により、暗号化したコンテンツをユーザに提供するデータ配信が行われている。

【0003】図10は、コンテンツ・プロバイダーが提供するコンテンツ及びそのコンテンツ鍵を、ユーザの受信装置まで配信する流れを示したものである。

【0004】暗号化されていないコンテンツ（例えば音楽データ、映像データ、書籍等の文書データ、静止画データ等）を保持するコンテンツ・プロバイダー101は、自己が保持する又は生成したコンテンツ鍵でコンテンツを暗号化し、これをサービス・プロバイダー102に供給する。また、コンテンツ・プロバイダー101は、コンテンツ鍵を、鍵管理センター103にも供給する。このコンテンツ鍵は、コンテンツ毎に違うものを用いても良いし、同じものでも良い。

【0005】鍵管理センター103は、自己の保持する配送用鍵（ユーザ毎に全て異なる鍵にしても良いし、全て共通でも良い）でこのコンテンツ鍵を暗号化する。鍵管理センター103は、ユーザからの要求に応じて、この配送用鍵により暗号化したコンテンツ鍵を供給する。

【0006】ユーザが持つ受信装置104は、衛星通信やケーブル通信、インターネット等を介して、サービス・プロバイダー102から、コンテンツ鍵により暗号化されたコンテンツを受信する。コンテンツを受信したユーザは、このコンテンツを楽しむために暗号を解かなくてはならない。このため、受信装置104は、鍵管理センター103に復号用のコンテンツ鍵を要求する。鍵管理センター103は、コンテンツ鍵の送信要求があると、このコンテンツ鍵を受信装置104に送信する。このとき、鍵管理センター103は、課金処理も同時に行う。この課金処理は、鍵管理センター103に登録されたユーザの銀行口座から料金を引き落としとしても良いし、ユーザからクレジットカード番号を送信してもらいこのカード番号に従って課金しても良い。また、受信装置104に備え付けられたICカードに蓄えられているプリペイドから必要な料金を引き落としとしても良い。この課金処理によりユーザは、コンテンツに関する権利を取得したことになる。

【0007】暗号化されたコンテンツ鍵を受信したユーザは、受信装置104の内部記憶装置111に保持されている配送用鍵でコンテンツ鍵を復号し、復号したコンテンツ鍵を用いて暗号化されたコンテンツを復号する。

【0008】ユーザは、この復号したコンテンツ鍵を、

50

独自に保持する保存用鍵で暗号化して外部記憶装置112に保存する。これは、コンテンツ鍵を配送するときに使った配送用鍵が一定期毎に変わる可能性があるためである。また、暗号化しないままコンテンツ鍵を保存することはコンテンツを暗号化しないで保存することと本質的に変わらず、他人に自由に内容を見られる可能性があるためである。また、ユーザは、自己が保持する保存用鍵でコンテンツ鍵を暗号化することにより、同一のコンテンツを復号する際に、再度課金されることなく使用することができる。そして、ユーザ独自の保存用鍵によりコンテンツ鍵を暗号化することにより、外部記憶装置112の内容が丸ごとコピーされることによる第3者の不正コピーを防止している。

【0009】

【発明が解決しようとする課題】ところで、コンテンツが記憶されている外部記憶装置112は故障によりアクセスできなくなる場合がある。このように外部記憶装置112にアクセスできなくなってしまうと、コンテンツを復号することができなくなってしまう。また、このコンテンツに関する権利を買い取っていることから再度課金しなければ二度と同一のコンテンツを得ることができなくなる。

【0010】これを避けるため、ユーザは、図11に示すように、受信装置104に第2の外部記憶装置113を設けて、外部記憶装置（以下、第1の外部記憶装置と言い換える。）112の内容を丸ごとコピーしておくことが考えられる。いわゆるバックアップといわれるものである。しかし、何ら制限なくバックアップを許可することは、コンテンツ鍵の無制限の使用を招いてしまうおそれがある。

【0011】例えば、コンテンツ鍵は、コンテンツ鍵の使用回数、使用時間等の条件を含む使用許諾情報とともに暗号化されている場合に、自由にコンテンツ鍵のバックアップが取られると、その条件を元に戻してしまう場合があり、これによりコンテンツ鍵が無制限に使用されてしまうことになる。例えば、使用回数が減ったデータに未使用のデータを上書きすることにより、使用回数の情報がもとに戻せる場合がある。なお、使用時間の条件とは、例えば、初めて利用してから何日間は使用可とする等といった条件である。

【0012】このように、何ら制限なくバックアップを許可することは、コンテンツ鍵の無制限の使用を招いてしまい、好ましくない。この対策として、例えば、図12に示すように、第1及び第2の外部記憶装置112、113毎に異なる書き換え不可能な識別情報（ID）を記憶装置内に持たせ、この識別情報と保存用鍵とを用いてコンテンツ鍵を暗号化する方法が考えられる。そして、第1の外部記憶装置112から第2の外部記憶装置113に対するコンテンツ及びコンテンツ鍵の複製は上述した図11のようにして内容を丸ごとコピーしてお

く。

【0013】ここで、識別情報を用いて行うコンテンツ鍵の復号については次のようになる。コンテンツ鍵は、まず識別情報から取り出した鍵（なお、識別情報そのものを鍵にしても良い）で暗号化され、続けて保存用鍵により暗号化される。この暗号化処理は、コンテンツ鍵を Kc 、保存用鍵を Ks 、ID1を第1の外部記憶装置の識別情報及びID2を第2の外部記憶装置の識別情報としたとき、次式により示すことができる。

【0014】 $K1 = Enc(Kc, ID1)$

$K2 = Enc(K1, Ks)$

ここで、“ $Enc(a, b)$ ”は、()内のデータ a をデータ b を用いてする暗号化処理を示し、すなわち、ここで得られる $K2$ が第1及び第2の外部記憶装置113に保存されている状態の暗号化されているコンテンツ鍵になる。

【0015】そして、コンテンツ鍵の復号について、受信装置104は、第1の外部記憶装置112から読み出したデータにより次式に示す処理を行う。

【0016】 $K1 = Dec(K2, Ks)$

$Kc = Dec(K1, ID1)$

ここで、“ $Dec(c, d)$ ”は、()内のデータ c をデータ d を用いてする復号処理を示す。このような処理により、受信装置104は、第1の外部記憶装置112に記憶されていたデータに基づいて正しくコンテンツ鍵 Kc を取り出すことができる。

【0017】一方、第2の外部記憶装置113から取り出したデータによりコンテンツ鍵を復号しようとした場合には、次式に示す処理が実行される。

【0018】 $K1 = Dec(K2, Ks)$

$Kc' = Dec(K1, ID2)$

ここで識別情報ID2により復号対象とされる $K1$ は上述したように $K1 = Enc(Kc, ID1)$ であるから、正しく Kc を取り出せない。すなわち、第2の外部記憶装置113から読み出した識別情報は識別情報ID2であり、また、識別情報は書き換えられないことから、正しく Kc を取り出せなくなる。

【0019】このような処理ではコンテンツ鍵の無制限なバックアップを防ぐことはできるが、今度はバックアップを取ったコンテンツ鍵による復旧ができなくなる。

【0020】そこで、本発明は、上述した実情に鑑みてなされたものであり、コンテンツの不正コピーを防止しながらその複製（バックアップ）を生成することを可能にするコンテンツ管理方法及びコンテンツ記憶システムの提供を目的としている。

【0021】

【課題を解決するための手段】本発明に係るコンテンツ管理方法は、上述の課題を解決するために、第1の保存用鍵により暗号化されたコンテンツ鍵と、コンテンツ鍵により暗号化されているコンテンツとを記憶している第

10

20

30

40

50

9

1のコンテンツ記憶手段の当該暗号化されているコンテンツ鍵を第1の保存用鍵により復号し、復号した得たコンテンツ鍵を、新たに生成した第2の保存用鍵により暗号化し、第2の保存用鍵により暗号化されたコンテンツ鍵と上記暗号化されているコンテンツとを第2のコンテンツ記憶手段に記憶する。

【0022】このようなコンテンツ管理方法は、第1のコンテンツ記憶手段に記憶されているコンテンツ鍵を第1の保存用鍵により復号する。そして、コンテンツ管理方法は、この復号して得たコンテンツ鍵を新たに生成した第2の保存用鍵により暗号化して第2のコンテンツ記憶手段に記憶する。

【0023】すなわち、コンテンツ管理方法は、第1のコンテンツ記憶手段に記憶されていたコンテンツ鍵を、新たに生成した第2の保存用により暗号化しなおし、第2のコンテンツ記憶手段に記憶することにより、第1のコンテンツ記憶手段に記憶されているコンテンツ鍵のバックアップを第2のコンテンツ記憶手段に取る。

【0024】また、本発明に係るコンテンツ記憶システムは、上述の課題を解決するために、第1の保存用鍵により暗号化されたコンテンツ鍵と、コンテンツ鍵により暗号化されているコンテンツとを記憶している第1のコンテンツ記憶手段と、データ及び鍵データを復号する復号手段と、データ及び鍵データを暗号化する暗号手段と、保存用鍵を生成する保存用鍵生成手段と、復号手段において第1の保存用鍵により復号した得たコンテンツ鍵を、保存用鍵生成手段により生成した第2の保存用鍵により暗号手段において暗号化して得た暗号化されたコンテンツ鍵と、暗号化されているコンテンツとを記憶する第2のコンテンツ記憶手段と、保存用鍵が記憶されて

いる保存鍵記憶手段とを備える。

【0025】このような構成を有するコンテンツ記憶システムは、第1のコンテンツ記憶手段に記憶されているコンテンツ鍵を第1の保存用鍵により復号する。そして、コンテンツ記憶システムは、この復号して得たコンテンツ鍵を新たに生成した第2の保存用鍵により暗号化して第2のコンテンツ記憶手段に記憶する。

【0026】すなわち、コンテンツ記憶システムは、第1のコンテンツ記憶手段に記憶されていたコンテンツ鍵を、新たに生成した第2の保存用により暗号化しなお

*40

$$Ca = IDa + (\text{その他の情報}) + Kpa + Siga \quad \dots (1)$$

この式(1)におけるSigaは、以下の式(2)のよ

$$Siga = Enc(Hash(IDa + (\text{その他の情報}) + Kpa), Ksc) \quad \dots (2)$$

この式(2)において、“Hash()”は、ハッシュ関数と呼ばれる一方向性関数である。このハッシュ関数は、データ長が長いデータを所定のビット長のデータに圧縮する関数で、出力からは入力わかりにくい関数であり、例えば、MD5やSHA-1等がある。“+”は、データを連結することを意味する。例えば、16ビ

ットデータ+16ビットデータとは、連続して並べて32ビットデータにすることを意味する。“Enc()”は、暗号化処理を表し、ここでは公開鍵暗号(例えばRSA暗号)を使用すると仮定する。ユーザBの公開鍵Kpbの正当性を示すための証明書Cbも、この証明書Caと同様である。すなわち、

10

*し、第2のコンテンツ記憶手段に記憶することにより、第1のコンテンツ記憶手段に記憶されているコンテンツ鍵のバックアップを第2のコンテンツ記憶手段に取る。

【0027】

【発明の実施の形態】以下、本発明を適用した実施の形態について、図面を参照しながら説明する。まず、本発明を適用した実施の形態の説明において使用する用語や処理内容等について説明する。

【0028】コンテンツとは、ディジタルデータになりうる全ての情報で、その情報自体が価値を持っているものである。例えば、コンテンツとは、音楽データ、映像データ、書籍等の文書データ、静止画データ等である。

【0029】暗号アルゴリズムは、第三者に内容がわからないようにデータを暗号化するアルゴリズムであればどのようなアルゴリズムであっても良い。例えば、暗号アルゴリズムとしては、公開鍵暗号方式や共通鍵暗号方式が一般に知られている。公開鍵暗号方式は、暗号化に使用する鍵と復号に使用する鍵とが異なる暗号アルゴリズムであり、例えばRSA暗号や、楕円曲線暗号が知られている。この公開鍵暗号方式では、2つの鍵の内、一般に公開される鍵が公開鍵、ユーザが秘密に保持している鍵が秘密鍵と呼ばれる。一方、共通鍵暗号方式は、暗号化する際に使用する鍵と復号する際に使用する鍵が同じである暗号アルゴリズムであり、例えばDES暗号や、FEAL(NTT)、Misty(三菱電機)等が知られている。この共通鍵暗号方式では、使用する鍵が共通鍵と呼ばれる。

【0030】ここで、ユーザAとユーザBとが、公開鍵暗号により互いに正当な相手であるか相互認証する場合について、図1を用いて説明する。

【0031】なお、ユーザAの公開鍵をKpa、秘密鍵をKsa、識別情報をIDaとする。また、ユーザBの公開鍵をKpb、秘密鍵をKsb、識別情報をIDbとする。そして、認証局の公開鍵をKpc、秘密鍵をKscとする。

【0032】また、ユーザAの公開鍵Kpaの正当性を示すための証明書Caは、以下の式(1)のようになる。

【0033】

$Cb = IDb + (\text{その他の情報}) + Kpb + Sigb$
である。なお、“Dec ()”は、復号処理を表す。

【0034】相互認証は、図1に示すステップS1からステップS4の手順により行われる。なお、ユーザA及びユーザBは、自らの鍵や識別情報の他に、自己の公開鍵の証明書Ca、Cbと認証局の公開鍵Kpcを保持している。

【0035】まず、ステップS1において、ユーザAは、乱数R1を生成する。そして、以下の式(3)に示すように、この乱数R1をKsaで暗号化し、R2を生成する。そして、Ca及びR2をユーザBに送る。

$$R2 = Enc(R1, Ksa) \quad \dots (3)$$

【0036】続いて、ステップS2において、ユーザBは、ユーザAから送られてきた証明書Ca (= Ida + (その他の情報) + Kpa + Siga) が正しいかどうか検証する。ユーザBは、まず、 $D1 = Hash(Ida + (\text{その他の情報}) + Kpa)$ を生成する。そして、このD1とDec(Siga, Kpc)とを比較し、一致していればKpaは正当であると判断する。

【0037】ユーザBは、Kpaが正当であると判断すると、以下の式(4)に示すように、R2をKpaで復号して、R1を生成する。

$$R1 = Dec(R2, Kpa) \quad \dots (4)$$

次に、以下の式(5)に示すように、このR1をKsbで暗号化し、R3を生成する。そして、上述したCb及びR3をユーザAに送る。

【0038】

$$R3 = Enc(R1, Ksb) \quad \dots (5)$$

【0039】続いて、ステップS3において、ユーザAは、ステップS2と同様にユーザBから送られてきた証明書Cbの検証を行い、Kpbが正当であるか判断する。ユーザAは、Kpbが正当であると判断すると、以下の式(6)に示すように、R3をKpbで復号化してR4を生成し、このR4とR1とを比較する。

【0040】

$$R4 = Dec(R3, Kpb) \quad \dots (6)$$

R1とR4とが一致していれば、ユーザBはKsbを持っていることになり、ユーザBの正当性が確認できる。もし、一致していなければ、ユーザBはCbを盗み見た不正者であると判断できる。次に、以下の式(7)に示すように、ハッシュ関数を用いて、R1とR2とからR5を生成する。

$$R5 = Hash(R1, R2) \quad \dots (7)$$

そして、以下の式(8)に示すように、このR5をKsaで暗号化し、R6を生成する。そして、R6をユーザBに送る。

$$R6 = Enc(R5, Ksa) \quad \dots (8)$$

【0041】続いて、ステップS4において、ユーザBは、以下の式(9)に示すように、ハッシュ関数を用いて、R1とR2からR7を生成する。

$$R7 = Hash(R1, R2) \quad \dots (9)$$

次に、以下の式(10)に示すように、送られてきたR6をKpaで復号してR8を生成する。

$$R8 = Dec(R6, Kpa) \quad \dots (10)$$

そして、R7とR8とを比較し、一致していればユーザAはKsaを持っていることになり、Aの正当性が確認できる。もし、一致していなければ、ユーザAはCaを盗み見た不正者であると判断できる。

【0042】以上のように、ユーザAとユーザBとは、両者が互いに正当であることを確認し合う相互認証を行うことができる。なお、乱数R1などのデータをその場限りの一時的な鍵として使用することがあり、この鍵のことをセッション鍵と呼ぶ。

【0043】内部記憶装置は、受信装置内に組み込まれた耐タンパー性のあるシングルチップIC内のメモリ(フラッシュメモリ、EEPROM等)や、受信装置とデータの授受ができるICカード等、第三者が簡単に中身を確認できないような記憶媒体であればどのようなものであっても良い。

【0044】外部記憶装置は、ハードディスク、光ディスク、テープメディア、半導体メモリ等のどのような記憶媒体や記憶装置等であっても良い。なお、これらの外部記憶装置には、それぞれを識別するための識別情報(ID)が書き込まれていても良く、この識別情報は書き換え不能になっていることが好ましい。

【0045】また、暗号化されたコンテンツのバックアップに関しては、このデータは、第三者からもらっても良いし、自由に複製しても良い。これは、暗号化されたコンテンツそのものはコンテンツ鍵がなければ使用することができないからである。

【0046】外部記憶装置に記憶される暗号化されたコンテンツ鍵は、この鍵データの中に、コンテンツを復号するための復号鍵の他に、この鍵を使用するための使用許諾情報、料金、使用回数等の情報が含まれ、また、コンテンツ(或いはコンテンツ鍵)を買い取った受信装置の識別情報も含まれている。ここで、使用回数とは、コンテンツ鍵の使用回数を制限する情報であって、例えば、コンテンツ鍵を復号できる回数であり、復号した際にその数が減らされる。

【0047】コンテンツの復号処理は、以上説明したコンテンツ鍵の暗号化を解き、使用条件等を取り出して、この使用条件に応じて暗号化されたコンテンツを復号することになる。例えば、コンテンツを10回だけ復号可能であるという使用回数の条件であれば、コンテンツ鍵を1回復号する毎にコンテンツ鍵に付随する使用条件の使用回数を減らす。また、例えばコピー禁止であるという条件があれば、他の機器へコンテンツのコピーをしようとした場合には、コンテンツの復号を行わないようなコピーが制限される。

【0048】次に、本発明を適用した実施の形態について

13

て説明する。図2に、このデータ配信システムのブロック構成図を示す。

【0049】本発明を適用した第1の実施の形態のデータ配信システムは、図2に示すように、暗号化されていないコンテンツを保持するコンテンツ・プロバイダー11と、コンテンツ・プロバイダー11が保持するコンテンツを衛星通信やケーブル通信、インターネット等を介してユーザに提供するサービス・プロバイダー12と、コンテンツ鍵の管理や提供したコンテンツの課金処理等を行う鍵管理センター13と、コンテンツを視聴等するユーザが持つ受信装置14とから構成される。また、この受信装置14は、その内部に内部記憶装置21を有し、その外部に外部記憶装置22が接続されている。

【0050】このデータ配信システムにおいて、コンテンツ・プロバイダー11から提供されたコンテンツが、ユーザの受信装置14の外部記憶装置22に記憶されるまでの手順について、この図2を参照しながら説明する。

【0051】暗号化されていないコンテンツを保持するコンテンツ・プロバイダー11は、図示しない乱数生成器でコンテンツ鍵（例えば共通鍵）を生成し、このコンテンツ鍵でコンテンツを暗号化する。次に、コンテンツ・プロバイダー11は、鍵管理センター13から供給された配送用鍵（例えば共通鍵、公開鍵であっても良い）を用いて、コンテンツ鍵及び使用許諾情報等のその他の情報を暗号化する。そして、コンテンツ・プロバイダー11は、これらの暗号化したコンテンツ及び暗号化したコンテンツ鍵をサービス・プロバイダー12に供給する。

【0052】ユーザが持つ受信装置14は、衛星通信やケーブル通信、インターネット等を介してサービス・プロバイダー12から暗号化されたコンテンツ及びコンテンツ鍵を受信する。これらを受信したユーザは、このコンテンツを楽しむためには暗号を解かなくてはならない。そのために、ユーザは、復号された状態のコンテンツ鍵を次のように入手する。

【0053】受信装置14は、暗号化されたコンテンツ鍵を直接鍵管理センター13に送信する。このとき暗号化されたコンテンツ鍵を一度外部記憶装置22に記憶しても良く、また、しなくても良い。すなわち、ユーザは、コンテンツ鍵の暗号化に使用している配送用鍵を持っておらず、このままではユーザはコンテンツ鍵を復号できないので、このコンテンツ鍵を一旦鍵管理センター13に送信する。このとき、受信装置14の識別情報や自己の保存用鍵も一緒に送信する。これらを受信した鍵管理センター13は、自己の保持する配送用鍵でコンテンツ鍵を復号し、ユーザから受け取った保存用鍵で再度暗号化する。その後、鍵管理センター13は、ユーザの識別情報に従って課金処理を行い、保存用鍵で暗号化したコンテンツ鍵を返送する。

14

【0054】これらのデータは、そのまま伝送しても良いし、相互認証で確立されたセッション鍵で暗号化した上で送っても良い。セッション鍵によりコンテンツ鍵等を暗号化する場合、ユーザは、保存用鍵を鍵管理センター13に送信しなくても良い。この場合、ユーザは、セッション鍵で暗号化されたコンテンツ鍵等を受信した後、このセッション鍵を用いてコンテンツ鍵等を一旦復号し、自己の持つ保存用鍵で暗号化する。

【0055】コンテンツ鍵を受信した受信装置14は、保存用鍵により暗号化されたコンテンツ鍵を外部記憶装置22に保存する。受信装置14の内部記憶装置21には、保存用鍵が保存されているため、いつでもコンテンツ鍵を復号することができ、また、このコンテンツ鍵を用いてコンテンツの復号ができる。なお、図2中には、外部記憶装置22や内部記憶装置21に各1つずつしか鍵を記載していないが、実際には数多くの暗号化されたコンテンツやコンテンツ鍵を保存していても良い。

【0056】以上のように、本発明を適用したコンテンツ配信システムでは、コンテンツ・プロバイダー11が有するコンテンツをコンテンツ鍵で暗号化してユーザに提供することができるとともに、このコンテンツを暗号化したコンテンツ鍵も暗号化してユーザに提供することができる。そして、ユーザは、提供されたコンテンツ鍵を復号して、コンテンツを復号することが可能となる。

【0057】なお、鍵管理センター13の課金処理は次の1～3の処理が考えられる。

1 識別情報に関係付けられた口座番号やクレジットカード番号を保持しておき、この番号に応じて銀行やカード会社から代金を徴収する。

2 鍵を送る毎に口座番号やクレジットカード番号を併せて送らせ決済する。

3 受信装置14の内部の内部記憶装置21に蓄えられた電子マネーから代金を引く。

【0058】また、このデータ配信システムにおいては、図3に示すように、受信装置14の内部記憶装置21に配送用鍵を予め保持させておき、この配送用鍵を用いてコンテンツ鍵を復号しても良い。この場合、ユーザは、配送用鍵を用いて復号したコンテンツ鍵を、自己が独自に保持する保存用鍵で暗号化しなおして外部記憶装置22に保存する。更に、コンテンツ鍵を復号する毎にログ情報を作成し、このログ情報を内部記憶装置21に蓄積する。そして、課金は、一定期間経過した後で所定回数の配送用鍵の復号を行った時や配送用鍵の更新を行った時等に、鍵管理センターにログ情報を送信することにより、処理される。

【0059】なお、このように内部記憶装置21に配送用鍵を予め保存しておく場合には、サービス・プロバイダー12が使用する配送用鍵は一定期間（例えば1ヶ月）毎に更新され、ユーザもそれに応じて鍵管理センター13から配送用鍵が供給されるものとする。つまり、

15

配送用鍵は、全てのユーザに対して共通であるため、安全性を鑑み時々変更する。

【0060】次に、図4に示すように、受信装置14に第2の外部記憶装置31を備えて、この第2の外部記憶装置31に対して外部記憶装置（以下、第1の外部記憶装置と言換える。）22に記憶されているコンテンツ鍵の複製、すなわちバックアップを取る手順について説明する。

【0061】このデータ配信システムにおいて、受信装置14は、データ及び鍵データを復号する復号手段31と、データ及び鍵データを暗号化する暗号化手段32と、保存用鍵が記憶されている保存用鍵記憶手段である内部記憶装置21とを内部に備えている。そして、受信装置14は、第1のコンテンツ記憶手段として第1の外部記憶装置22と、第2のコンテンツ記憶手段として第2の外部記憶装置23とを備えている。ここで、受信装置14は、例えば、耐タンパー性を持ったICチップで構成されている。そして、この受信装置14内にある内部記憶装置21は、例えば、ICチップ内のフラッシュメモリとして、また、復号手段31及び暗号手段32は、ASICやプログラムにより実現される。

【0062】第1の外部記憶装置22は、第1の保存用鍵により暗号化されているコンテンツ鍵と、コンテンツ鍵により暗号化されているコンテンツとを記憶するコンテンツ記憶手段である。また、第2の外部記憶装置23は、復号手段31において第1の保存用鍵により復号して得たコンテンツ鍵を、乱数生成器34により生成した第2の保存用鍵により暗号手段32において暗号化して得た暗号化されたコンテンツ鍵と、暗号化されているコンテンツとを記憶するコンテンツ記憶手段である。

【0063】そして、第1及び第2の外部記憶装置22、23には、書き換え不可能なデータとしてこの第1及び第2の外部記憶装置22、23それぞれに固有に付された識別情報ID1、ID2が記憶されている。

【0064】また、第1の外部記憶装置22は、例えば、IEEE1394インターフェースを備えたハードディスクにより構成されている。また、第2の外部記憶装置23は、IEEE1394インターフェースを備えた光ディスクドライブ及びメディアにより構成されている。ここで、第1及び第2の外部記憶装置22、23が例えばハードディスクである場合には、上述した識別情報は、ROMの中に書き込んでおき、特殊なコマンドがきた際に読み出されるようにしておけば良いし、光ディスク等の場合には、書き換え不能なトラックに記憶しておくようにする。

【0065】また、このデータ配信システムにおいて、鍵管理センター13は、保存用鍵を生成する保存用鍵生成手段である乱数生成器34と、生成した保存用鍵と、この保存用鍵により暗号化されるコンテンツが記憶されるコンテンツ記憶手段である外部記憶装置の識別情報を

16

保存する保存手段である記憶装置35とを備えている。ここで、記憶装置35には、例えば、管理用鍵やこの鍵管理センター13において生成した第2の保存用鍵等の各種鍵が保存されている。

【0066】このように構成されるデータ配信システムについて、受信装置14が第1の外部記憶装置22に記憶されているコンテンツ鍵のバックアップを取る際の手順に沿って説明する。

【0067】ユーザは、買い取ったコンテンツ鍵のバックアップを作ろうとした際には、まず、鍵管理センター13に第2の保存用鍵を要求する。ここで第2の保存用鍵の要求は保存用鍵要求コマンドを送信することにより行い、この保存用鍵要求コマンドには、例えば、受信装置14の識別番号、バックアップデータを保存する第2の外部記憶装置の識別情報ID2等が含まれている。

【0068】この保存用鍵要求コマンドを受信した鍵管理センター13は、乱数生成器34で第2の保存用鍵を生成する。そして、鍵管理センター13は、送られてきた第2の外部記憶装置23の識別情報ID2とこの第2の保存用鍵を記憶装置35に保存し、その一方、この第2の保存用鍵を受信装置14に返送する。鍵管理センター13は、この時、ユーザの受信装置14の識別情報に従って課金処理を行っても良い。なお、この処理は、どちらかと言えば登録といった意味合いが強く、その場合には、登録処理を行っても良い。また、鍵管理センター13と受信装置14との通信経路はインターネット、ケーブル回線、電話回線等いずれでも良い。

【0069】受信装置14は、鍵管理センター13から送信されてきたこの第2の保存用鍵を用いて第1の外部記憶装置22に記憶されているコンテンツ鍵のバックアップを取る。図5には、コンテンツのバックアップを取る際の第1の外部記憶装置22に記憶されているコンテンツ鍵に対して行う処理の流れを具体的に示している。

【0070】第2の保存用鍵を受け取った受信装置14は、第1の外部記憶装置22からコンテンツ鍵を読み出しその復号を行う。コンテンツ鍵の復号は、具体的には、内部記憶装置21に保存してある第1の保存用鍵で復号し（図5中（A）から図5中（B）に示す処理）、そして、第1の外部記憶装置22の識別情報ID1で復号するといった処理（図5中（B）から図5中（C）に示す処理）により実行する。

【0071】そして、受信装置14は、復号して得たコンテンツ鍵を今度は暗号化して第2の外部記憶装置23に記憶する。コンテンツ鍵を暗号化して第2の外部記憶装置23に記憶する処理は、具体的には、第2の外部記憶装置23の識別情報ID2で暗号化し（図5中（C）から図5中（D）に示す処理）、先に鍵管理センター13から受け取っている第2の保存用鍵で暗号化して第2の外部記憶装置23に保存する（図5中（D）から図5中（E）に示す処理）。

【0072】なお、このように、各外部記憶装置にコンテンツ鍵を暗号化するには、保存用鍵とコンテンツ鍵が記憶される外部記憶装置の識別情報を用いて暗号化しているが、以降の説明では、識別情報による暗号化の説明を省略する。なお、図面における表示も以降省略する。

【0073】以上の手順により第2の外部記憶装置23に対して第1の外部記憶装置22に記憶されていたコンテンツ鍵のバックアップが取られる。これにより、第三者等により不正な複製を行うことを防止するとともに、第1の外部記憶装置22内にあるコンテンツ鍵のバックアップを安全に取ることができる。そして、鍵管理センター13では、バックアップの要求に対して、すなわち、第2の保存用鍵の生成要求により、受信装置14のユーザに対する課金処理を行うこともできるようになる。

【0074】ここで説明したバックアップの処理は基本的な例であり、次により具体的な例について説明する。

【0075】上記第2の保存用鍵に基づいて第3の保存用鍵を生成してコンテンツのバックアップを取ること10もできる。なお、第2の保存用鍵の生成についても、上述した実施の形態では第2の保存用鍵を鍵管理センター13から受け取っているが、図6に示すように、受信装置14に乱数生成器41を設けて、この乱数生成器41により第2の保存用鍵を生成することもできる。このように生成された第2の保存用鍵を、受信装置14は、内部記憶装置21内にある鍵管理センター13の公開鍵により暗号化することにより第3の保存用鍵を得て、この第3の保存用鍵を第2の外部記憶装置23に保存する。

【0076】また、図7に示すように、受信装置14が鍵管理センター13に第2の保存用鍵の要求をすることによりこの鍵管理センター13から受け取った第2の保存用鍵に基づいて、受信装置14が公開鍵を用いて第3の保存用鍵を生成することもできる。

【0077】このように、鍵管理センター13の公開鍵により第2の保存用鍵を暗号化することにより、コンテンツ鍵のバックアップは自由に作れるものの、それを復旧するには鍵管理センター13の秘密鍵が必要になる。よって、鍵管理センター13では、これを利用する、すなわち第3の保存用鍵を復号するアクセスがあった際に課金処理を行うことができるようになる。

【0078】また、第3の保存用鍵についても鍵管理センター13において生成することもできる。この場合、鍵管理センター13は、上述したように乱数生成器34により第2の保存用鍵を生成すると共に、記憶装置35に保持している管理用鍵でこの第2の保存用鍵を暗号化して第3の保存用鍵を生成する。そして、鍵管理センター13は、受信装置14にこの第3の保存用鍵を第2の保存用鍵と併せて送り、受信装置14では、この第3の保存用鍵を第2の外部記憶装置23に保存する。

【0079】なお、受信装置14において第3の保存用鍵を生成する場合は、鍵管理センター13の公開鍵を用いて第3の保存用鍵を生成しているが、鍵管理センター13において第3の保存用鍵を生成する場合には、管理用鍵として公開鍵又は共通鍵のいずれを用いることができる。これは、例えば、受信装置14において第3の保存用鍵の生成に共通鍵を使用した場合、内部記憶装置21にこの鍵がそのまま持たれていることになるため、悪質な第三者の攻撃対象になってしまうからであり、これ10に対し、鍵管理センター13で保存する鍵は、第三者の攻撃対象になりたくないため、どちらの形態の鍵でも使用することができるからである。すなわち、通常、受信装置14はユーザが所持していること、鍵管理センター13はシステム管理会社が保持していることから、アクセスの自由度、装置の分解等の可能性について違いがあるためである。

【0080】このように、第2の外部記憶装置23に記憶する第3の保存用鍵を鍵管理センター13において生成することにより、バックアップを自由な生成をできなくすることが可能になる。また、鍵管理センター13では全てのユーザの第2の保存用鍵を管理する必要がないため、負担も軽減される。

【0081】また、上述したように第3の保存用鍵を生成した場合については、第2の保存用鍵を削除することもできる。すなわち、上述したように、鍵管理センター13から第3の保存用鍵を受け取った後、又は受信装置14内で第3の保存用鍵を生成した後に、バックアップデータ作成の確認により第2の保存用鍵を削除する。

【0082】このように、使用し終えた第2の保存用鍵を削除することにより、バックアップは、鍵管理センター13との課金処理が終了しなければその復旧ができなくなる。例えば、受信装置14は、コンテンツ鍵の復旧が必要になった際に、鍵管理センター13に第2の保存用鍵の送信を要求する。コンテンツ鍵の復旧は、例えば、バックアップとして取っておいてコンテンツ鍵が何らかの事情で必要になった場合、例えば、第1の外部記憶装置22が故障して動作しなくなってしまう場合に行われる。

【0083】鍵管理センター13に対する第2の保存用鍵の要求については、具体的には、受信装置14は、第2の外部記憶装置23の識別情報に基づいて鍵管理センター13から第2の保存用鍵を要求する。すなわち、受信装置14は、第2の外部記憶装置23から識別情報ID2を読み出し、受信装置14の識別情報と一緒に鍵管理センター13に送信する。これを受信した鍵管理センター13は、第2の外部記憶装置23の識別情報に従って内部記憶装置35から第2の保存用鍵を探し出し、これを受信装置14に送り返す。このように第2の保存用鍵を受信装置14に送信する一方で、受信装置14では、受信装置14の識別情報から所定の課金処理を行40

19

う。ここで言う課金方法は、先に説明しているように行う。

【0084】また、受信装置14は、上述したように、第3の保存用鍵を生成して第2の保存用鍵を削除した場合において、第3の保存用鍵に基づいて第2の保存用鍵を取得することができる。この処理について図10を用いて説明する。

【0085】受信装置14は、第3の保存用鍵を鍵管理センター13に送信する(図8中(1)及び(2)の処理)。なお、第3の保存用鍵は、上述したように、第2の保存用鍵を鍵管理センター13の公開鍵又は管理用鍵(これも鍵管理センター13の公開鍵と同一とする)で暗号化されたものである。また、受信装置14は、この第3の保存用鍵と共に受信装置14、第2の外部記憶装置23それぞれの識別情報を一緒に送信することもできる。

【0086】これを受信した鍵管理センター13は、記憶装置35に保持している秘密鍵で復号して第2の保存用鍵を得る(図8中(3)の処理)。そして、鍵管理センター13は、この第2の保存用鍵をセッション鍵で暗号化する(図8中(4)の処理)。ここで、セッション鍵は、例えば、鍵管理センター13と受信装置14がデータのやりとりを行う前に行った相互認証時に確立されているものである。

【0087】そして、鍵管理センター13は、このデータ(セッション鍵により暗号化している第2の保存用鍵)を受信装置14に返送する。鍵管理センター13は、この第2の保存用鍵を返送した際に所定の課金処理を行う。

【0088】受信装置14は、鍵管理センター13が保持しているセッション鍵と同一のセッション鍵を所持しており、例えば内部記憶装置21に記憶しており、このセッション鍵により鍵管理センター13から送信されてきたデータを復号して第2の保存用鍵を生成する(図8中(6)の処理)。そして、この第2の保存用鍵によりコンテンツ鍵が復元される(図8中(7)の処理)。

【0089】このように、鍵管理センター13の公開鍵等で暗号化した第3の保存用鍵を鍵管理センター13に送信し、鍵管理センター13ではこの第3の保存用鍵により第2の保存用鍵を生成することにより、鍵管理センター13の負担を軽くした上でコンテンツ鍵の復旧ができるようになる。

【0090】また、受信装置14は、第2の外部記憶装置23に第1の外部記憶装置22に記憶されているコンテンツ及びコンテンツ鍵のバックアップを取る際に、受信装置14の識別情報も第2の外部記憶装置23に記憶しておくこともできる。これにより、所定の受信装置においてのみ復旧作業を行うことができる。

【0091】この場合、受信装置14は、復旧作業の際に、第2の外部記憶装置23から受信装置の識別情報を

20

読み出し、この受信装置の識別情報の検査結果に応じて、具体的には復旧作業を行っている受信装置と同一であるかどうか検証してもし異なっていた場合に、復旧作業を行わないようにすることができる。

【0092】また、受信装置14は、復旧したコンテンツ鍵の使用許諾情報に、この鍵が復旧されたコンテンツ鍵であるという情報を付加することもできる。これにより、受信装置14は、復旧したコンテンツ鍵を第1の外部記憶装置22に移動しようとした際に、読み出されたコンテンツ鍵の使用条件に復旧されて旨の情報(例えば、"復旧鍵"であるといった情報)が付加されている場合、移動先、例えば、他の外部記憶装置に保存されているのコンテンツ鍵とを比較することができるようになる。この比較結果に基づいて、移動先に保存されているコンテンツ鍵が同一である時にエラー処理する等することにより、合法的にバックアップを作成して、コンテンツ鍵を復旧させて複数のコンテンツ鍵を同一記憶装置に持たせることを防ぐことができるようになる。

【0093】また、コンテンツ鍵の使用回数を制限する使用回数情報をコンテンツ鍵に付加することもできる。これは、使用回数の減ったコンテンツ鍵が、復旧作業によりその回数が元に戻ってしまうことを防ぐためである。すなわち、これにより、受信装置12は、使用回数が減ったコンテンツ鍵のバックアップを取らないようにすることができる。

【0094】また、受信装置14は、第1の外部記憶装置22の識別番号ID1を第2の外部記憶装置23にバックアップしたコンテンツ鍵と共に保存しておくこともできる。これにより、故障したはずの第1の外部記憶装置22を再度接続することによるコンテンツ鍵の複製を防ぐことができる。例えば、次のような処理を行うことにより実現される。

【0095】まず、受信装置14は、第1の外部記憶装置22の識別番号ID1をバックアップしたコンテンツ鍵と共に第2の外部記憶装置23に保存する。そして、受信装置14は、コンテンツ鍵の復旧作業を行った際に、第2の外部記憶装置23に記憶している第1の外部記憶装置22の識別番号ID1を受信装置14の内部記憶装置21に移動して保存する。それから、第1の外部記憶装置22のコンテンツ鍵の復号の要求があった際に、受信装置14は、この要求があった当該第1の外部記憶装置22の識別情報と自己が保持している復旧作業済みの第2の外部記憶装置23より得たバックアップ元の外部記憶装置の識別信号とを比較した比較結果に基づいてエラー処理する。

【0096】このように、受信装置14は、内部記憶装置21に記憶された識別番号を確認することで、復旧されたコンテンツ鍵を記憶している外部記憶装置に対してのアクセスをできないようにして、故障したはずの第1の外部記憶装置22を再度接続することによるコンテン

21

ツ鍵の複製を防ぐことができる。

【0097】なお、図9には、コンテンツ鍵及び使用許諾情報の例を示す。第1の例は、図9中(A)に示すように、鍵データが“01ABCF54”とされるコンテンツ鍵に、使用制限回数示す再生制限情報として“無制限”、コピー制限情報として“無制限”、及び出力情報として“アナログのみ”が付加されている。また、第2の例は、図9(B)に示すように、鍵データが“86945ABC”とされるコンテンツ鍵に、使用制限回数示す再生制限情報として“100回”、コピー制限情報として“アナログのみ”、及び出力情報として“デジタルSCMS付き”が付加されている。

【0098】

【発明の効果】本発明に係るコンテンツ管理方法は、第1の保存用鍵により暗号化されたコンテンツ鍵と、コンテンツ鍵により暗号化されているコンテンツとを記憶している第1のコンテンツ記憶手段の当該暗号化されているコンテンツ鍵を第1の保存用鍵により復号し、復号した得たコンテンツ鍵を、新たに生成した第2の保存用鍵により暗号化し、第2の保存用鍵により暗号化されたコンテンツ鍵と上記暗号化されているコンテンツとを第2のコンテンツ記憶手段に記憶することにより、第1のコンテンツ記憶手段に記憶されているコンテンツ鍵を第1の保存用鍵により復号し、この復号して得たコンテンツ鍵を新たに生成した第2の保存用鍵により暗号化して第2のコンテンツ記憶手段に記憶することができる。

【0099】すなわち、コンテンツ管理方法は、第1のコンテンツ記憶手段に記憶されていたコンテンツ鍵を、新たに生成した第2の保存用により暗号化しなおし、第2のコンテンツ記憶手段に記憶することにより、第1のコンテンツ記憶手段に記憶されているコンテンツ鍵のバックアップを第2のコンテンツ記憶手段に取ることができる。

【0100】このコンテンツ管理方法により、コンテンツの不正コピーを防止しながらその複製(バックアップ)を生成することが可能になる。

【0101】また、本発明に係るコンテンツ記憶システムは、第1の保存用鍵により暗号化されたコンテンツ鍵と、コンテンツ鍵により暗号化されているコンテンツとを記憶している第1のコンテンツ記憶手段と、データ及び鍵データを復号する復号手段と、データ及び鍵データを暗号化する暗号手段と、保存用鍵を生成する保存用鍵生成手段と、復号手段において第1の保存用鍵により復号した得たコンテンツ鍵を、保存用鍵生成手段により生成した第2の保存用鍵により暗号手段において暗号化して得た暗号化されたコンテンツ鍵と、暗号化されているコンテンツとを記憶する第2のコンテンツ記憶手段と、保存用鍵が記憶されている保存鍵記憶手段とを備えることにより、第1のコンテンツ記憶手段に記憶されているコンテンツ鍵を第1の保存用鍵により復号し、この復号

22

して得たコンテンツ鍵を新たに生成した第2の保存用鍵により暗号化して第2のコンテンツ記憶手段に記憶することができる。

【0102】すなわち、コンテンツ記憶システムは、第1のコンテンツ記憶手段に記憶されていたコンテンツ鍵を、新たに生成した第2の保存用により暗号化しなおし、第2のコンテンツ記憶手段に記憶することにより、第1のコンテンツ記憶手段に記憶されているコンテンツ鍵のバックアップを第2のコンテンツ記憶手段に取ることができる。

【0103】このコンテンツ記憶システムは、コンテンツの不正コピーを防止しながらその複製(バックアップ)を生成することを可能にする。

【図面の簡単な説明】

【図1】公開鍵暗号により互いに正当な相手であるか認証する認証処理について説明するための図である。

【図2】本発明の実施の形態であるコンテンツ配信システムのブロック図である。

【図3】本発明の実施の形態の他のコンテンツ配信システムのブロック図である。

【図4】コンテンツ配信システムの備える受信装置が第2の外部記憶装置を備えた際の構成を示すブロック図である。

【図5】鍵管理センターに対して受信装置が第2の保存用鍵を要求し、受信装置が受信した第2の保存用鍵を第2の外部記憶手段に記憶するときの手順を説明するために用いた図である。

【図6】受信装置が第2の保存用鍵を生成する乱数生成器を備えている構成を示すブロック図である。

【図7】受信装置が鍵管理センターの公開鍵により第2の保存用鍵を暗号化して第3の保存用鍵を生成したときの構成を示すブロック図である。

【図8】受信装置が、鍵管理センターにこの鍵管理センターの公開鍵により暗号化して得た第3の保存用鍵を送信して、第2の保存用鍵を得るときの手順を説明するために用いた図である。

【図9】コンテンツ鍵及び使用許諾情報の具体例を示す図である。

【図10】従来のコンテンツ配信システムのブロック図である。

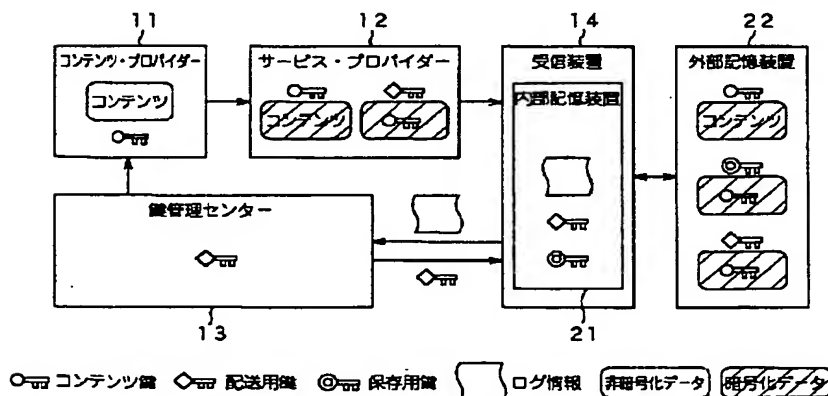
【図11】従来のコンテンツ配信システムの備える受信装置が第1の外部記憶装置の記憶しているコンテンツ鍵のバックアップを第2の外部記憶装置に取する場合の説明に用いた図である。

【図12】従来のコンテンツ配信システムの備える受信装置が第1の外部記憶装置の記憶しているコンテンツ鍵のバックアップを第2の外部記憶装置に取する場合において、外部記憶装置が自己の識別情報により暗号化及び復号化するときの説明に用いた図である。

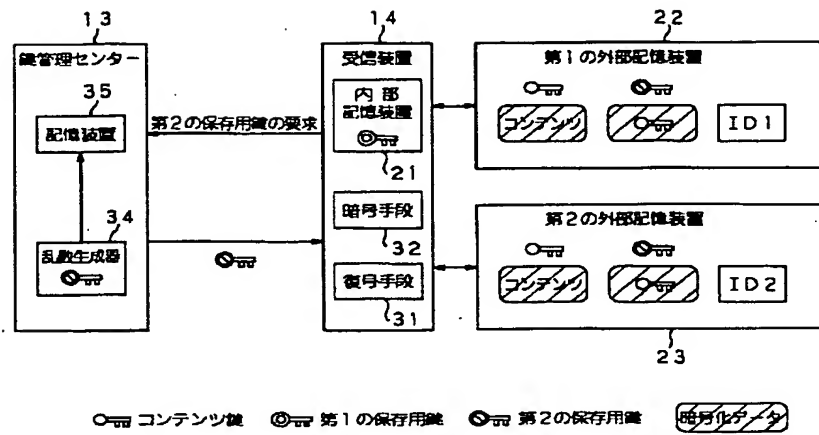
【符号の説明】

24

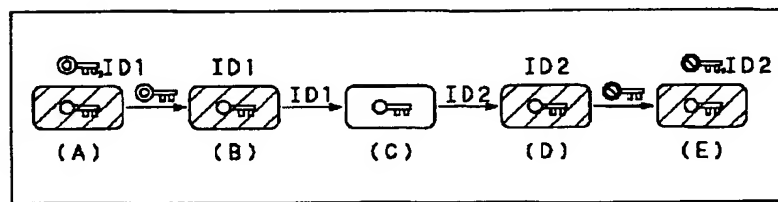
【図 1】



【図4】

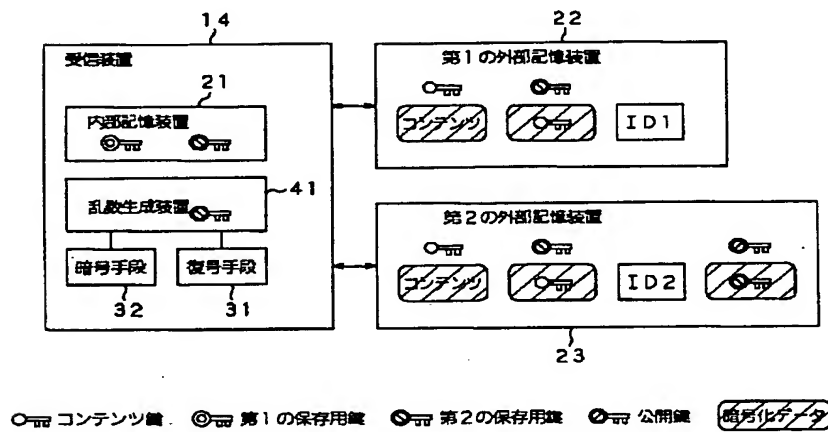


【図5】

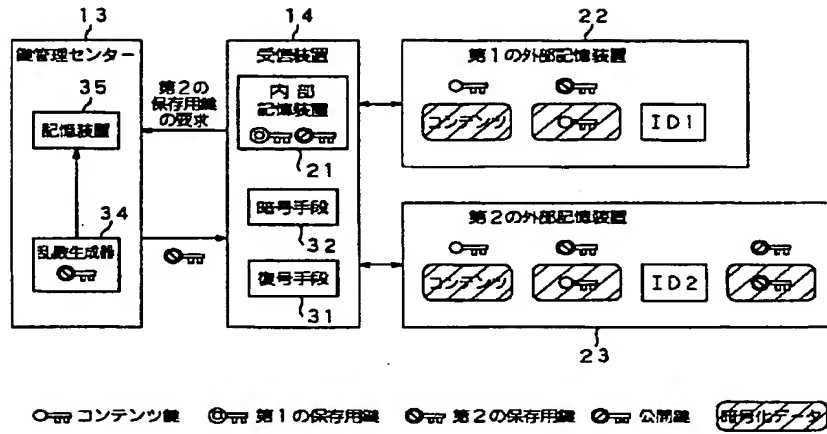


コンテンツ鍵 第1の保存用鍵 第2の保存用鍵 暗号化データ

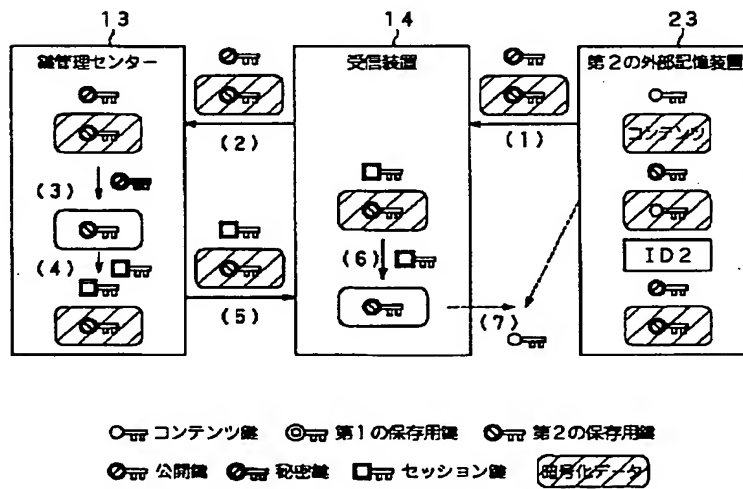
【図6】



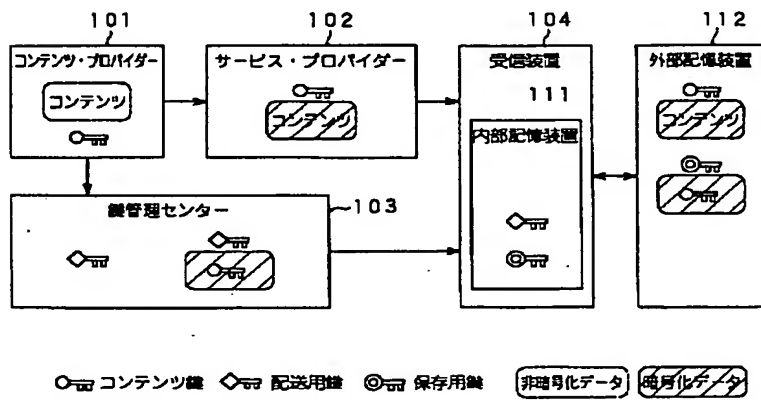
【図7】



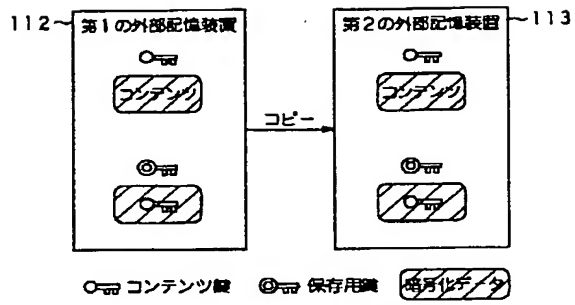
【図8】



【図10】



【図11】



【図12】

